KINGDOM OF SAUDI ARABIA
Northern Border University (NBU)
Journal of the North for Basic & Applied Sciences(JNBAS)
p - ISSN : 1658 -7022 / **e-ISSN:** 1658 - 7014
www.nbu.edu.sa
s.journal@nbu.edu.sa

Operational Security Exposure and Attack Surface Analysis of Password Manager Browser Extensions

Maryam Almarwani
Department of Cybersecurity, College of Computer Science and Engineering, Taibah University, Madinah, 42453, Saudi Arabia

(**Received:** :9th May 2026; **Accepted:** 8th June 2026)

Abstract
Password manager browser extensions have become widely used authentication tools for improving password security and reducing credential reuse across digital platforms. Despite the deployment of client-side encryption mechanisms, browser-integrated password managers may still introduce security exposure because of elevated browser permissions, runtime credential handling, synchronization behavior, and direct interaction with webpages and browser APIs.
This study analyzes the attack surface characteristics of password manager browser extensions operating in Chromium-based browser environments. The evaluation examines browser permissions, runtime interaction behavior, storage mechanisms, and synchronization-related communication patterns associated with browser-integrated password managers. To support structured analysis, the study adopts a multidimensional security evaluation framework integrating permission exposure analysis, runtime injection assessment, browser-side storage interaction analysis, and exploratory correlation analysis.
Experimental results obtained from seven widely used password manager browser extensions show measurable differences in exposure characteristics across the evaluated platforms. The findings suggest that password manager browser extensions rely on different integration strategies involving privileged browser permissions, runtime webpage interaction, browser-side persistence mechanisms, and synchronization-related communication behavior. The analysis additionally shows that encryption deployment alone does not fully eliminate runtime exposure within browsercentric authentication environments.

Keywords: Credential Protection; Autofill Exposure; Synchronization Complexity; Runtime Interaction; Browser APIs.

1658-7022© JNBAS. (1448 H/2026). Published by Northern Border University (NBU). All Rights Reserved.

(*) **Corresponding Author**:
Maryam Almarwani
Department of Cybersecurity, College of Computer Science and Engineering,
Taibah University, Madinah, 42453, Saudi Arabia

E-mail: mmmarwani@taibahu.edu.sa

DOI: 10.12816/0062624

1. Introduction

Password managers have become a widely adopted mechanism for improving authentication security and reducing password reuse across online services. In modern computing environments, these systems are commonly deployed as browser extensions that generate, store, synchronize, and automatically fill user credentials across multiple platforms. Their widespread adoption is largely driven by their ability to improve both security and usability while reducing the burden of managing large numbers of credentials (Wiefling, Jørgensen, Thunem, & Iacono, 2022; Alodhyani, Theodorakopoulos, & Reinecke, 2020; Jubur, Shrestha, & Saxena, 2025).

Although encryption remains a fundamental component of password-manager security, the protection of credentials increasingly depends on a broader set of operational safeguards. Modern authentication environments rely on secure interaction workflows, browser-side isolation mechanisms, credential-handling protections, and exposure-reduction strategies throughout the authentication lifecycle (P. Wang, Boodraj, & Baskerville, 2025; Saadi, Sadiq, Akif, & Farhan, 2024). Consequently, understanding the security posture of password managers requires evaluating not only how credentials are encrypted, but also how they are processed, accessed, and exposed during browser operation.

However, browser-integrated password managers also introduce new cybersecurity issues since they operate within highly dynamic environments of browsers and require high permissions to interact with webpages, browser APIs, autofill mechanisms, and browser sessions. Browser extensions often request additional permissions, which can increase exposure and security risk to the browser. Picazo et al. (Picazo-Sanchez, Ortiz-Martin, Schneider, & Sabelfeld, 2022) showed that many extensions do not follow the least privilege principle and Wang et al. (K. Wang et al., 2022) showed that malicious extensions can target sensitive data and user credentials in the browser.

Browser security and the risks associated with extensions have become an important cybersecurity concern as a result. Chalyi et al. (Chalyi, Driaunys, & Rudˇzionis, 2025) investigated the vulnerabilities of browsers with evaluation metrics based on CVE and highlighted the persistence of browser security weaknesses in modern environments. Jin et al. (Jin, Li, & Zou, 2024) investigated the operational impact of extensions on Chromium-based browser environments and demonstrated that browser extensions could have a significant impact on the browser's behaviour during runtime. Other studies concentrated on browserside protection mechanisms to defend against extension-based threats. Wang et al. (X. Wang, Du, Wang, Wang, & Fang, 2021) proposed WebEnclave, which leverages the software enclave concepts to safeguard sensitive web secrets from malicious browser extensions. Further studies also investigated browser extension abuse, privilege abuse and browser API exposure in modern browser ecosystems.

Recent studies have increasingly examined cybersecurity risk assessment, security exposure and structured security evaluation in modern digital systems (Ganin et al., 2020; Amro, Gkioulos, & Katsikas, 2023; Atlam, Azad, Alassafi, Alshdadi, & Alenezi, 2020; Cornwell, Bilson, Gepp, Stern, & Vanstone, 2022; Uddin, Mollah, Islam, & Ali, 2023). The significance of risk management, attack modelling and runtime exposure analysis, and dynamic cybersecurity evaluation across cyber-physical and digitally transformed environments was highlighted in existing studies (Amro et al., 2023; Uddin et al., 2023). Other work pointed to the importance of structured risk-oriented evaluation to understand the cybersecurity exposure in complex operational systems (Atlam et al., 2020; Cornwell et al., 2022).

Encryption alone, however, does not remove the security exposure; clientside encryption is widely deployed in password managers, but active browser sessions can leak sensitive information through runtime credential handling, memory exposure, autofill abuse, session persistence, and excessive browser permissions. Prior work indicated that, even with encryption mechanisms in place, processing on the browser side and interaction at runtime can provide other potential pathways for exposure (X. Wang et al., 2021). Previous work studied the attack surface of password managers, browser extensions or browser vulnerabilities separately, but not their combined attack surface in browser-based authentication environments.

In this study, attack surface is defined as the set of browser-accessible interaction pathways that may increase exposure during active extension operation. These pathways include privileged browser permissions, interaction with webpages at runtime, browser-session access, browser-side persistence mechanisms, synchronization-related communication behaviour, and extension interaction with browser APIs and webpages. Most of the current research focuses on individual topics like encryption design, malware detection, permission analysis, browser vulnerabilities, or authentication usability, but does not systematically evaluate the operational cryptographic exposure during runtime browser operation.

This study makes three contributions. First, it provides a multidimensional security analysis of password manager browser extensions. Second, it evaluates seven widely used extensions with respect to permissions, runtime interaction, storage behavior, and synchronization-

related communication. Third, it introduces a structured perspective for assessing browser-centric attack-surface exposure during password-manager operation.

Therefore, in this study we provide an attack surface and operational cryptographic risk analysis of password manager browser extensions. The work focuses on assessing operational exposure associated with browser permissions, runtime credential management, autofill activity, synchronisation processes, session persistence, and browser-extension interaction. The study also provides a structured view to assess the cryptographic exposure of browser-based password management systems.

2. Related Work

2.1 Password Manager Security

Password managers have been broadly studied as mechanisms to enhance password security, decrease password reuse, and encourage secure authentication practices on digital platforms. Existing studies have shown that password managers improve password management behaviour, improve credential organization, and simplify authentication workflows while reducing unsafe password practices (Wiefling et al., 2022; Alodhyani et al., 2020; Jubur et al., 2025). Other studies highlighted the importance of usability, transparency, operational trust, and user-centred protection in password manager adoption and authentication effectiveness (Alodhyani et al., 2020; P. Wang et al., 2025).

Several studies also investigated vulnerabilities associated with authentication systems, password storage, and browser-integrated authentication environments. Saadi et al. (Saadi et al., 2024) discussed vulnerabilities in graphical password systems and different protection approaches for authentication security. Previous studies additionally examined browser-integrated password managers, credential accessibility, runtime interaction, and browser-related dependencies (Jubur et al., 2025; Wiefling et al., 2022; P. Wang et al., 2025). Other works explored cybersecurity awareness, user perception, and behavioural security practices associated with authentication systems and operational digital environments (Kennison & Chan-Tin, 2020; Moustafa, Bello, & Maurushat, 2021).

Recent research also examined security implications associated with authentication technologies and machine-learning-driven security systems (Bitton et al., 2021). Existing studies further indicated that complexity, privacy concerns, and runtime exposure remain important considerations in modern authentication infrastructures (Petronio & Child, 2020; Senna, Reis, Castro, & Dias, 2020).

Most previous studies focused on usability, trust, and credential protection. Less attention has been given to the combined impact of permissions, runtime interaction, storage behavior, and synchronization mechanisms on operational security exposure.

2.2 Browser Extension Security

Browser extensions have become an important cybersecurity research area because of their elevated privileges and direct interaction with browser APIs, webpages, browser sessions, and sensitive user information. Picazo et al. (PicazoSanchez et al., 2022) investigated whether Chrome extensions comply with the principle of least privilege and reported that many extensions request excessive permissions beyond operational requirements. Existing studies also examined browser extension abuse, browser API exposure, runtime interaction risks, and extension-related threats within browser ecosystems (Zahid, Inayat, Daneva, & Mehmood, 2021).

Malicious browser extensions have attracted increasing research attention in recent years. Wang et al. (K. Wang et al., 2022) analyzed cryptocurrencythemed malicious browser extensions and showed that browser extensions can be used to steal credentials and sensitive browser information through deceptive behaviours. Other studies discussed browser-related exposure, manipulation techniques, runtime browser interaction risks, and extension abuse concerns associated with browser-integrated environments (Petronio & Child, 2020; Smart, Sood, & Vaccaro, 2022).

Several studies explored browser security from broader operational and defensive perspectives. Chalyi et al. (Chalyi et al., 2025) analyzed browser vulnerabilities using CVE-based security metrics and highlighted the persistence of browser-side vulnerabilities in modern browser environments. Jin et al. (Jin et al., 2024) examined the operational impact of browser extensions on Chromiumbased browser environments and showed that browser extensions may significantly influence runtime browser behaviour and browser performance. Wang et al. (X. Wang et al., 2021) proposed WebEnclave to protect browser-side secrets from malicious browser extensions using software enclave concepts. Additional studies discussed browser privacy exposure, browser-side uncertainty, interaction risks, and runtime browser manipulation associated with modern browser-centric platforms (Smart et al., 2022; Petronio & Child, 2020).

Existing studies additionally emphasized that browser extensions significantly contribute to attack surface expansion because of privileged interaction with webpages, browser APIs, synchronization mechanisms, and browser-session operations (Picazo-Sanchez et al., 2022; K. Wang et al., 2022).

Existing research has mainly examined permissions, malicious extensions, or browser vulnerabilities separately. A broader evaluation that combines these dimensions remains relatively limited.

2.3 Operational and Cybersecurity Risk Analysis

Cybersecurity evaluation has become increasingly important in modern digital and cyber-physical environments. Ganin et al. (Ganin et al., 2020) proposed a multicriteria framework for cybersecurity risk assessment and operational security management, while Atlam et al. (Atlam et al., 2020) reviewed adaptive risk-based access control approaches for dynamic security evaluation in modern computing systems. Additional studies emphasized the importance of structured operational cybersecurity assessment, uncertainty evaluation, and management, and automated cybersecurity analysis mechanisms in modern digital infrastructures (Eckhart et al., 2022). Additional studies investigated cybersecurity exposure associated with machine learning systems and operational decision-making mechanisms (Bitton et al., 2021).

Recent works further highlighted the importance of runtime exposure evaluation, operational attack modeling, and structured cybersecurity assessment across browser-centric and distributed operational systems (Cheng, Cai, Wang, Dong, & Li, 2026). While these studies provide valuable cybersecurity-evaluation methodologies, they are generally designed for broader operational environments rather than browser-integrated authentication ecosystems. As a result, their direct applicability to password-manager browser extensions remains limited.

2.4 Research Gap

The existing literature confirms that password managers, browser extensions, browser vulnerabilities, and cybersecurity mechanisms introduce multiple security and operational challenges. However, most prior studies analyze these components separately. Existing works mainly focus on password usability, authentication trust, browser extension permissions, malware detection, browser vulnerabilities, or general cybersecurity risk assessment.

Current literature provides limited analysis of the combined security exposure associated with browser-integrated password manager extensions, particularly in relation to runtime credential handling, browser-session interaction, autofill behaviour, synchronization mechanisms, and attack surface expansion. Existing studies also lack structured evaluation frameworks that integrate browser permissions, extension behaviour, browser interaction, runtime exposure, and cryptographic deployment within unified browser security analysis environments.

This study addresses this gap by presenting an attack surface and security risk analysis framework for password manager browser extensions based on runtime exposure assessment and structured cybersecurity evaluation.

Existing research has mainly examined permissions, malicious extensions, or browser vulnerabilities separately. A broader evaluation that combines these dimensions remains relatively limited.

Cybersecurity evaluation has become increasingly important in modern digital and cyber-physical environments. Ganin et al. (Ganin et al., 2020) proposed a multicriteria framework for cybersecurity risk assessment and operational security management, while Atlam et al. (Atlam et al., 2020) reviewed adaptive risk-based access control approaches for dynamic security evaluation in modern computing systems. Additional studies emphasized the importance of structured operational cybersecurity assessment, uncertainty evaluation, and runtime exposure analysis in digital infrastructures (Chandna & Tiwari, 2021; Eckhart, Ekelhart, & Weippl, 2022).

Other studies investigated security exposure and cyber risk assessment in digitally transformed infrastructures and cyber-physical systems. Amro et al. (Amro et al., 2023) applied ATT&CK-based methodologies for cyber risk assessment and operational security analysis in cyber-physical environments. Amro et al. (Amro & Gkioulos, 2022) additionally explored threat-informed cyber risk management strategies in autonomous systems.

Existing literature also discussed operational exposure, adaptive security

Table 1: Comparison Between Prior Studies and the Proposed Framework

Study	Permission Analysis	Runtime Interaction Analysis	Communication Exposure Evaluation	Storage Unified
Picazo et al. (Picazo-Sanchez et al., 2022)	✓	–	–	–
Wang et al. (K. Wang et al., 2022)	✓	✓	–	–
Jin et al. (Jin et al., 2024)	–	✓	–	–
Wang et al. (X. Wang et al., 2021)	–	✓	–	–
Proposed Study	✓	✓	✓	✓

Table 1 highlights that most previous studies focused on isolated aspects of browser extension security such as permission analysis, runtime interaction, or browser-side protection mechanisms. Unlike these studies, the proposed framework evaluates permission exposure, runtime interaction behavior, storage interaction mechanisms, and synchronization-related communication characteristics within a unified operational exposure perspective. This integrated view enables a broader assessment of browser-centric attack-surface expansion in passwordmanager environments.

3. Methodology

This study adopts a cybersecurity evaluation methodology to analyze password manager browser extensions from an attack surface and security exposure perspective. The methodology focuses on how browser permissions, runtime credential handling, browser-extension interaction, synchronization behavior, and browser-session operations contribute to security exposure during active browser sessions. Existing studies showed that browser extensions operate with elevated browser privileges and may significantly influence browser behavior, runtime interaction, and browser-related exposure (Picazo-Sanchez et al., 2022; K. Wang et al., 2022; Jin et al., 2024).

The study evaluates seven browser-integrated password manager extensions deployed within Chromium-based browser environments. The evaluated extensions include Bitwarden, LastPass, Dashlane, NordPass, Proton Pass, Keeper, and RoboForm. These extensions were selected because of their widespread adoption, browser integration capabilities, synchronization functionality, and active interaction with authentication-related browser operations. Existing literature demonstrated that password managers improve authentication usability and credential management while also introducing browser-related dependencies and runtime interaction risks (Wiefling et al., 2022; Alodhyani et al., 2020; Jubur et al., 2025; P. Wang et al., 2025).

The security analysis pipeline consisted of several sequential stages. First, the evaluated password manager extensions were collected from the Chrome Web Store as Chromium extension packages (CRX format). Second, the CRX packages were extracted and analyzed to identify manifest permissions, optional permissions, host permissions, content scripts, browser-side storage interaction, and synchronization-related communication references. Third, runtime characteristics including injected JavaScript behavior, browser-session interaction patterns, browser-side persistence mechanisms, and external communication exposure were evaluated. Finally, exploratory correlation analysis was conducted to investigate relationships between permission exposure, runtime interaction behavior, browser-side storage mechanisms, and synchronization-related communication behavior across the evaluated extensions.

The methodology combines concepts from browser security analysis, operational cybersecurity risk evaluation, and runtime exposure assessment (Ganin et al., 2020; Atlam et al., 2020; Cornwell et al., 2022). Additional studies also emphasized the importance of adaptive cybersecurity evaluation, uncertaintyaware security analysis, and operational risk-oriented assessment within digitally transformed infrastructures and distributed operational systems (Gupta, Shankar, Lai, & Kumar, 2023; Eckhart et al., 2022; Uddin et al., 2023). These perspectives support the use of exposure analysis for evaluating browser-integrated authentication systems and runtime security behavior.

The security analysis pipeline was implemented using automated Pythonbased analysis scripts for CRX extraction, manifest parsing, browser permission identification, content-script inspection, storage-reference extraction, and synchronization-related URL analysis. The automated analysis process was designed to improve consistency, reproducibility, and structured operational comparison across the evaluated browser extensions. To improve reproducibility, all extension packages were extracted and analyzed using identical Chromiumbased environments and standardized parsing procedures. The automated analysis workflow applied consistent manifest extraction, permission identification, storage-reference analysis, and runtime interaction inspection across all evaluated extensions.

Table 2: Extracted Operational Features Used in the Security Analysis

Feature Category	Extracted Features
Permission Exposure	Manifest permissions, optional permissions, host permissions
Runtime Interaction	Content scripts, injected JavaScript files, webpage match patterns
Sensitive Browser Access	Clipboard access, scripting permissions, tab interaction permissions
Storage Interaction	localStorage references, sessionStorage references, IndexedDB interaction, chrome.storage usage
Communication Exposure	External URL references, synchronization-related communication indicators
Operational Indicators	Runtime interaction scope, browser-session interaction behavior

The analysis focuses on browser permissions, runtime credential handling, autofill operations, browser-session persistence, extension-browser interaction, synchronization mechanisms, and communication

behavior associated with password manager browser extensions.

Unlike prior studies that focused on isolated aspects of password-manager security, the proposed framework evaluates permission exposure, runtime interaction behavior, storage interaction mechanisms, and synchronization-related communication characteristics within a unified operational exposure perspective.

Table 2 summarizes the primary operational browser-security features extracted during the experimental evaluation. The selected features support structured comparative analysis across browser permissions, runtime interaction behavior, browser-side persistence mechanisms, and synchronization-related communication exposure.

Browser permissions were evaluated because previous studies demonstrated that excessive browser permissions may violate least privilege principles and significantly expand browser attack surfaces (Picazo-Sanchez et al., 2022). Additional works discussed browser interaction risks, malicious extension behavior, and runtime exposure pathways associated with browser ecosystems (K. Wang et al., 2022; Asif, Lodhi, Sarwar, & Ashfaq, 2023; Zahid et al., 2021).

The study also investigates security exposure associated with client-side encryption deployment in browser-integrated password managers. Although encryption mechanisms protect stored credentials, previous studies indicated that runtime interaction and browser-side processing may still expose sensitive information during active browser sessions (X. Wang et al., 2021; Jubur et al., 2025). Existing literature additionally emphasized that runtime exposure, synchronization complexity, and browser-side interaction remain important cybersecurity concerns in modern authentication environments (Petronio & Child, 2020; Senna et al., 2020).

To support structured evaluation, this study adopts a structured security perspective for analyzing browser extension exposure. Prior studies highlighted the importance of structured cybersecurity assessment, operational resilience evaluation, and runtime exposure analysis in modern digital systems (Amro et al., 2023; Amro & Gkioulos, 2022; Chandna & Tiwari, 2021). Other works discussed adaptive cybersecurity management, AI-driven operational evaluation, and uncertainty-aware cybersecurity analysis in operational infrastructures (Butnaru, Mylonas, & Pitropakis, 2021; Eckhart et al., 2022). Based on these perspectives, the proposed methodology evaluates how browser permissions, extension behavior, runtime credential processing, synchronization mechanisms, and browser interaction collectively contribute to operational attack surface expansion in password manager browser extensions.

4. Threat Model

This study considers a browser-centric threat environment in which password manager browser extensions operate inside modern web browsers while interacting with webpages, browser APIs, browser sessions, synchronization services, and external communication channels. Browser-integrated password managers operate with elevated privileges and direct access to sensitive authenticationrelated information, making them important targets within browser ecosystems (Picazo-Sanchez et al., 2022; K. Wang et al., 2022).

The threat model assumes that attackers may exploit operational exposure associated with browser-extension interaction, excessive permissions, malicious webpages, runtime credential handling, synchronization mechanisms, or browser-side operational weaknesses. Existing studies demonstrated that malicious browser extensions and browser-side manipulation techniques may expose sensitive credentials and browser-related information through deceptive behaviors and runtime interaction mechanisms (K. Wang et al., 2022; Asif et al., 2023; Smart et al., 2022).

The model focuses primarily on security threats rather than direct cryptographic algorithm compromise. The analysis therefore emphasizes runtime exposure pathways associated with browser-session interaction, autofill operations, synchronization behavior, extension communication mechanisms, and browser API interaction. Previous research highlighted that runtime browser interaction and browser-side processing may introduce operational exposure even when strong encryption mechanisms are deployed (X. Wang et al., 2021; Jubur et al., 2025).

The study does not attempt to identify or exploit zero-day vulnerabilities, compromise commercial password manager infrastructures, bypass deployed cryptographic protections, or perform offensive penetration testing against evaluated products. Instead, the analysis focuses on exposure characteristics associated with browser permissions, runtime interaction behavior, browser-session processing, synchronization mechanisms, and browser-integrated attack surface expansion. All experimental evaluations were conducted within controlled local environments without interacting with real user credentials, compromising external infrastructures, or performing unauthorized offensive activities against commercial password management services.

The considered threat environment includes malicious webpages, browserside script injection, unauthorized browser-session access, extension compromise, clipboard

monitoring, synchronization abuse, runtime credential interception, and application-level exposure arising from browser-integrated authentication workflows. Existing studies additionally discussed operational uncertainty, browser-side manipulation risks, and adaptive runtime exposure associated with modern browser ecosystems and digital interaction environments (Petronio & Child, 2020).

The targeted assets include stored credentials, runtime decrypted credentials, browser-session information, autofill-related data, synchronization tokens, and authentication-related browser interaction data. These assets are considered highly sensitive because they directly influence authentication security, credential confidentiality, and browser security exposure. Previous studies emphasized that browser-integrated systems and browser extensions may significantly contribute to attack surface expansion because of privileged interaction with browser APIs, webpages, synchronization services, and operational browser mechanisms (Picazo-Sanchez et al., 2022; K. Wang et al., 2022; Jin et al., 2024). The experimental analysis did not involve human participants, real credential collection, unauthorized access attempts, or interaction with private user authentication data. All evaluations were conducted within controlled local environments using publicly available browser extension packages.

5. Experimental Design

The experimental design of this study focuses on evaluating password manager browser extensions from an operational cryptographic security perspective. The evaluation investigates how browser permissions, runtime credential handling, synchronization behavior, browser-session persistence, and extension-browser interaction contribute to security exposure during active browser operation.

The study evaluates widely used browser-integrated password manager extensions operating within Chromium-based browser environments. Browserbased password managers were selected because they directly interact with webpages, browser APIs, browser sessions, synchronization services, and autofill mechanisms while simultaneously handling highly sensitive authenticationrelated information. Existing literature confirmed that browser extensions may significantly influence browser operational behavior and runtime exposure because of elevated browser privileges and direct interaction with browser components (Jin et al., 2024; Picazo-Sanchez et al., 2022; K. Wang et al., 2022).

5.1 Dataset and Evaluated Extensions

The selected extensions were chosen according to their popularity, availability within the Chrome Web Store ecosystem, active maintenance status, and support for browser-based credential synchronization. The final dataset included seven password manager extensions spanning different vendors, synchronization architectures, permission configurations, and browser-integration approaches. The analysis focuses on seven widely used password manager browser extensions: Bitwarden, LastPass, Dashlane, NordPass, Proton Pass, Keeper, and RoboForm. These extensions were selected because of their widespread adoption, browser integration capabilities, synchronization functionality, and active interaction with authentication-related browser operations. In addition, they represent some of the most widely deployed password-manager browser extensions discussed in recent password-manager surveys and authentication studies (Jubur et al., 2025). This selection was intended to provide a representative cross-section of commonly used browser-based password-management solutions rather than focusing on a single vendor or architectural design.

The evaluated extensions were downloaded as Chromium extension packages (CRX format) and extracted within controlled experimental environments for security analysis. The experimental pipeline included manifest extraction, browser permission analysis, runtime interaction assessment, content-script evaluation, browser-side storage analysis, synchronization-related communication analysis, and exploratory correlation analysis. To improve experimental consistency, the operational extraction and browser-extension analysis procedures were repeated across controlled execution environments using identical Chromiumbased configurations and standardized extension analysis workflows.

The analysis specifically focused on extension operational behavior associated with browser permissions, injected scripts, browser-session interaction, browser-side persistence mechanisms, synchronization complexity, and runtime exposure. Existing literature emphasized that browser extensions may significantly contribute to browser attack surface expansion because of privileged interaction with webpages, browser APIs, browser sessions, and browser-side operational mechanisms (Picazo-Sanchez et al., 2022; K. Wang et al., 2022; Jin et al., 2024).

The experimental analysis focuses on evaluating browser permissions, operational browser interaction, runtime credential processing, browser-session behavior, synchronization mechanisms, and extension communication behavior associated with password manager browser extensions. Existing studies highlighted that excessive browser permissions and privileged browser interaction may significantly increase browser attack surface exposure and operational cybersecurity risks (Picazo-Sanchez et al., 2022; K. Wang et al., 2022). Additional works also emphasized runtime browser exposure, browser-side uncertainty, and interaction risks

associated with browser-centric digital environments (Petronio & Child, 2020).

The evaluation additionally investigates security exposure associated with client-side encryption deployment within password manager browser extensions.

Although encryption protects stored credentials, previous research demonstrated that runtime interaction and browser-side processing may still expose sensitive information during active browser sessions (X. Wang et al., 2021; Jubur et al., 2025). Existing literature further highlighted that synchronization complexity, browser-session persistence, and runtime credential handling remain important operational cybersecurity concerns in modern authentication systems (Senna et al., 2020; Gupta et al., 2023).

To support comparative analysis, the study evaluates operational exposure across seven password manager browser extensions using a structured operational cybersecurity perspective. The evaluation investigates how differences in browser permissions, synchronization architecture, runtime interaction mechanisms, and extension operational behavior influence operational attack surface expansion and runtime exposure characteristics. Previous studies emphasized the importance of structured operational cybersecurity assessment, adaptive security evaluation, and runtime exposure analysis within digitally transformed operational systems (Ganin et al., 2020; Atlam et al., 2020; Cornwell et al., 2022; Uddin et al., 2023).

6. Results and Security Analysis

This section presents the experimental findings obtained from the security analysis of password manager browser extensions. The evaluation was conducted within controlled Chromium-based browser environments using extracted CRX extension packages and browser-extension security analysis procedures. The experimental pipeline included manifest extraction, permission analysis, contentscript evaluation, browser-side storage assessment, synchronization-related communication analysis, and exploratory correlation analysis.

The evaluation focuses on browser permission exposure, runtime interaction behavior, browser-side storage interaction, synchronization-related communication behavior, and operational attack surface characteristics associated with browser-integrated password manager extensions.

6.1 Permission Exposure Analysis

The first stage of the analysis evaluated the browser permissions requested by each password manager extension after extracting and analyzing the corresponding CRX extension packages. The analysis focused on manifest permissions, optional permissions, and host permissions associated with runtime browser interaction and operational browser exposure.

The results indicate noticeable differences in permission exposure across the evaluated extensions. Table 3 summarizes the comparative operational exposure indices.

To support structured comparative evaluation, an operational exposure index was calculated using a weighted heuristic model integrating manifest permissions, optional permissions, and host permissions:

Table 3: Operational Exposure Index Across Password Manager Browser Ex-tensions

Extension	Permission	Optional	Host	Exposure Index
Bitwarden	16	2	2	20.0
Keeper	14	0	3	17.6
RoboForm	13	3	1	16.6
LastPass	12	2	2	16.0
Dashlane	12	1	2	15.2
Proton Pass	8	5	2	14.4
NordPass	10	2	2	14.0

$$\text{ExposureIndex} = (1.0 \times \text{Permission}) + (0.8 \times \text{Optional}) + (1.2 \times \text{Host})$$

To evaluate the robustness of the weighting strategy, a sensitivity analysis was additionally performed using alternative weighting configurations. The analysis was designed to determine whether the relative ranking of extensions remained stable under different reasonable weighting assumptions.

Host permissions were assigned slightly higher weights because they directly influence webpage interaction scope and external browser exposure surfaces, while optional permissions were weighted lower because they may not always be activated during routine browser operation. The exploratory sensitivity analysis indicated

that the overall ordering of extensions remained broadly consistent across alternative weighting configurations. Minor variations were observed only among extensions with similar exposure scores, while the highest- and lowestranked extensions remained unchanged. These observations provide additional confidence that the reported exposure trends are not solely dependent on a single weighting configuration.

Table 3 shows that Bitwarden demonstrated the highest operational exposure index among the evaluated extensions, followed by Keeper and RoboForm. NordPass exhibited the lowest overall exposure index, while LastPass, Dashlane, and Proton Pass occupied intermediate positions. The results indicate measurable variation in permission-related exposure across the seven evaluated password-manager extensions.

The findings indicate that password manager extensions frequently require elevated browser privileges to support synchronization, autofill functionality, runtime credential handling, and browser integration operations.

The results are consistent with previous studies highlighting that browser extensions may request excessive permissions beyond minimal operational requirements (Picazo-Sanchez et al., 2022). The analysis additionally confirms that browser exposure cannot be evaluated solely based on encryption deployment because browser permissions significantly influence attack surface characteristics during runtime browser operation.

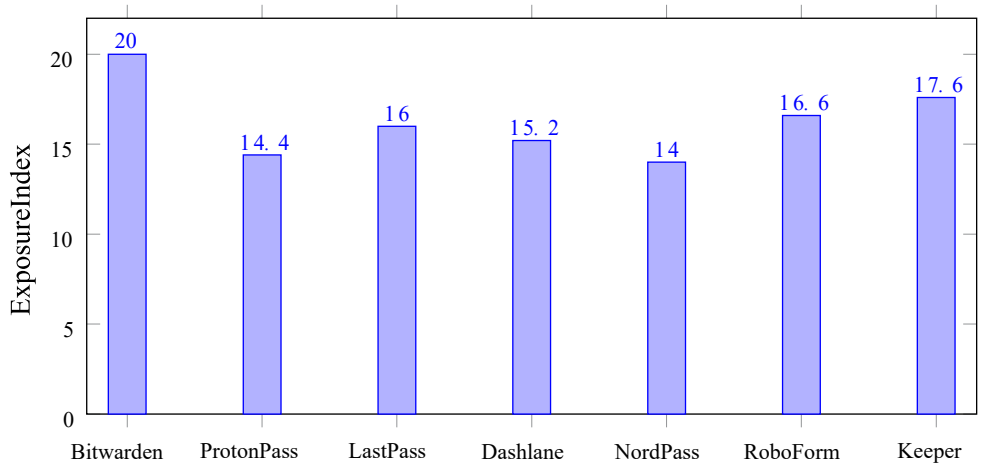

Figure 1: Comparative Operational Exposure Index Across Seven Password Manager Extensions

Figure 1 illustrates the comparative operational exposure distribution across the evaluated extensions immediately following the permission analysis results.

The expanded evaluation demonstrates that exposure characteristics vary considerably across commercially deployed password-manager extensions. Although Bitwarden exhibited the highest overall permission-related exposure score, Keeper and RoboForm also demonstrated relatively elevated exposure levels, suggesting that browser-integration strategies differ substantially across vendors.

6.2 Runtime Injection and Browser Interaction Exposure

The second stage of the analysis evaluated runtime webpage interaction exposure through content-script deployment and injected JavaScript behavior extracted from the evaluated CRX extension packages. Browser content scripts directly interact with webpages and therefore contribute to runtime exposure and browser attack surface expansion. Injected JavaScript activity refers to extension-associated runtime scripts deployed into webpages during browser interaction. Match patterns represent webpage scope definitions extracted from extension manifests and used to determine operational webpage interaction coverage. Table 4 presents the runtime interaction characteristics observed across the evaluated password manager browser extensions.

Table 4 demonstrates substantial variation in runtime interaction behavior across the evaluated extensions. NordPass exhibited the broadest webpage matching scope with 13 match patterns, while Dashlane demonstrated the highest content-script deployment and injected JavaScript activity. In contrast, Bitwarden, Proton Pass, and RoboForm relied on comparatively smaller runtime interaction footprints.

These findings indicate that exposure is multidimensional and cannot be measured exclusively through permission counts. Although Bitwarden demonstrated

Table 4: Runtime Injection and Browser Interaction Exposure

Extension	Content Scripts	Injected JS	Match Patterns
Dashlane	6	8	9
NordPass	5	6	13
LastPass	4	4	7
Keeper	2	3	7
Bitwarden	2	2	4
Proton Pass	2	2	4
RoboForm	2	2	2

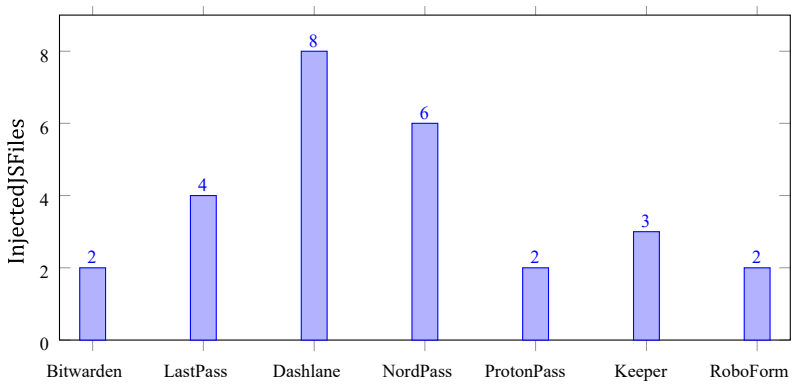

Figure 2: Injected JavaScript Exposure Across Seven Password Manager Extensions

The highest permission-related exposure index, Dashlane and NordPass exhibited considerably broader runtime interaction characteristics. Proton Pass showed relatively high permission exposure while maintaining a comparatively limited runtime interaction footprint. This observation suggests that different extensions rely on distinct architectural and browser-integration strategies within Chromium-based environments.

The results further support previous discussions regarding runtime browser interaction exposure and operational browser-side risks associated with browser extensions (Jin et al., 2024; K. Wang et al., 2022). Figure 2 visualizes the distribution of injected JavaScript activity across the evaluated extensions.

The expanded evaluation confirms that runtime exposure characteristics do not necessarily correlate with permission exposure levels. Extensions with moderate permission scores may still exhibit extensive runtime webpage interaction through content-script deployment and injected browser-side functionality.

Table 5: Sensitive Permission Exposure

Extension	Sensitive Permission Count
Bitwarden	11
Dashlane	9
LastPass	9
NordPass	8
Proton Pass	8
RoboForm	7
Keeper	7

6.3 Sensitive Permission Analysis

The analysis additionally evaluated the presence of sensitive browser permissions associated with browser monitoring, runtime interaction, scripting, clipboard access, and browser-session exposure. The evaluated permissions were identified through manifest analysis of the extracted browser-extension packages.

Table 5 summarizes the sensitive permission distribution across the evaluated extensions.

As shown in Table 5, Bitwarden demonstrated the highest number of sensitive permissions among the evaluated extensions. Dashlane and LastPass followed with nine sensitive permissions each, while NordPass and Proton Pass exposed eight sensitive permissions. RoboForm and Keeper exhibited the lowest counts among the evaluated extensions. The evaluated sensitive permissions included clipboard access, scripting capabilities, tab interaction, browser monitoring permissions, and runtime communication permissions.

The findings indicate that password manager extensions consistently rely on privileged browser interaction to support autofill operations, credential synchronization, runtime webpage integration, and browser-session management. However, elevated permission sensitivity may simultaneously increase operational attack-surface exposure and browser dependency during active execution.

Figure 3 illustrates the comparative distribution of sensitive browser permissions observed during the Chromium-based security analysis.

The expanded evaluation demonstrates that sensitive browser permissions are common across modern password-manager extensions. Although the absolute counts vary, all evaluated extensions required multiple permissions associated with browser interaction, scripting, or credential-related functionality, indicating that privileged browser access remains an inherent characteristic of browser-integrated password-management systems.

6.4 Browser-Side Storage Interaction Analysis

The experimental analysis further evaluated browser-side storage interaction behavior associated with password manager browser extensions extracted from Chromium-compatible CRX packages. The analysis focused on storage references, local storage interaction, IndexedDB usage, and browser-side persistence

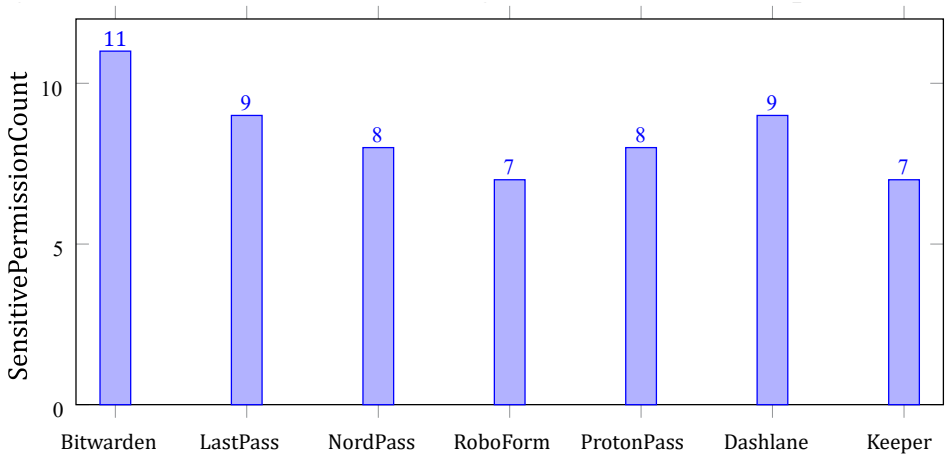

Figure 3: Sensitive Browser Permission Distribution Across Seven Password Manager Extensions

Table 6: Browser-Side Storage Interaction Analysis mechanisms identified within browser-extension operational components.

Extension	Storage	localStorage	sessionStorage	indexedDB	chrome.storage
Bitwarden	368	37	0	1	45
LastPass	207	175	16	16	10
Dashlane	565	60	39	36	41
NordPass	294	10	18	61	0
Proton Pass	260	36	0	12	0
Keeper	621	2	46	60	66
RoboForm	269	6	8	2	0

Table 6 summarizes the browser-side storage interaction characteristics observed during the experimental analysis.

Table 6 demonstrates substantial variation in browser-side storage interaction across the evaluated extensions. Keeper exhibited the highest overall storage-reference activity, while LastPass demonstrated the highest localStorage interaction frequency. NordPass showed the highest IndexedDB interaction activity, closely followed by Keeper. The results indicate that browser-integrated password managers employ substantially different persistence and browser-side storage architectures.

These observations indicate that password manager extensions rely on different browser-side persistence and storage strategies. Some extensions appear to emphasize browser-managed storage mechanisms, whereas others exhibit heavier reliance on local persistence references or IndexedDB-based interaction. The findings additionally suggest that browser interaction complexity differs substantially across browser-integrated password-manager architectures.

The results further support previous discussions regarding runtime exposure, browser-side operational interaction, and synchronization complexity in

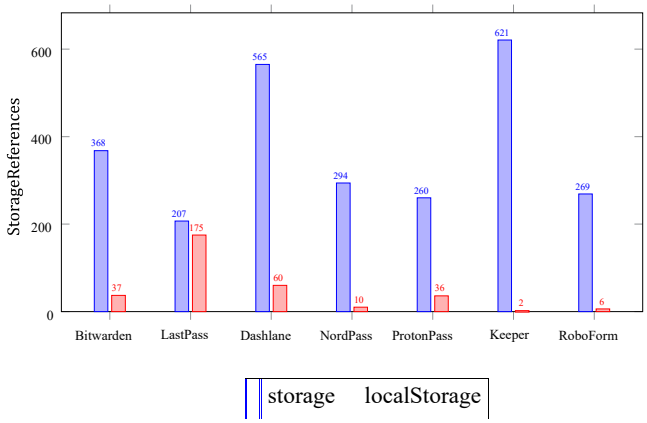

Figure 4: Browser-Side Storage Interaction Behavior Across Seven Password Manager Extensions

browser-centric authentication systems (Petronio & Child, 2020; Senna et al., 2020). Figure 4 presents the comparative browser-side storage interaction behavior across the evaluated extensions.

The expanded seven-extension evaluation reinforces the observation that browser-side storage behavior varies considerably across password-manager implementations. While some extensions demonstrate extensive storage interaction activity, others rely on more limited browser-side persistence footprints, highlighting architectural diversity in credential-management and synchronization strategies.

6.5 External Communication Exposure

The analysis additionally evaluated external communication complexity by identifying unique URL references associated with browser-extension operational interaction and synchronization behavior extracted from Chromium-based extension environments.

The results presented in Table 7 indicate substantial variation in external communication complexity across the evaluated extensions. RoboForm demonstrated the largest number of unique URL references, followed by Keeper, NordPass, and Dashlane. In contrast, Proton Pass exhibited the smallest number of external communication references. These findings suggest notable differences in synchronization architecture, external service integration, and operational.

Table 7 summarizes the external communication exposure characteristics identified during the security analysis.

Extension	Unique URLs Found
RoboForm	1065
Keeper	570
NordPass	507
Dashlane	445
Bitwarden	241
LastPass	235
Proton Pass	102

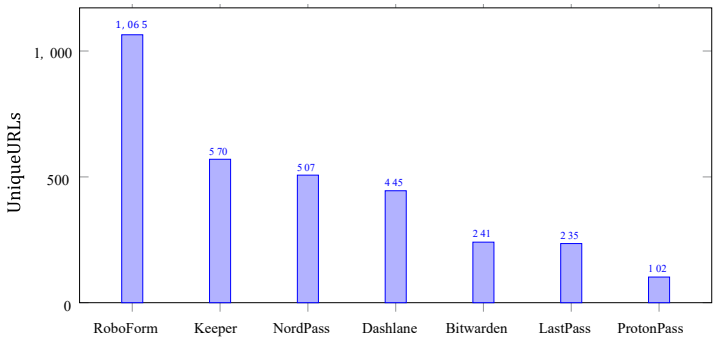

Figure 5: External Communication Exposure Across Seven Password Manager Extensions
interaction surfaces within browser-integrated environments.

The findings do not necessarily indicate insecure communication behavior. However, broader external interaction references may increase operational communication complexity and expand synchronization-related exposure pathways within browser ecosystems.

Figure 5 illustrates the comparative external communication exposure observed across the seven evaluated password manager browser extensions.

The expanded evaluation reveals that communication exposure varies considerably among password-manager implementations. Extensions with larger numbers of external communication references may rely on broader synchronization infrastructures, telemetry services, cloud integration components, or external authentication mechanisms. These observations further highlight the diversity of browser-extension operational architectures across modern passwordmanagement ecosystems.

6.6 Exploratory Correlation Analysis

The final stage of the experimental evaluation investigated exploratory operational relationships between permission exposure, runtime interaction behavior, browser-side storage interaction, and synchronization-related communication behavior within Chromium-based browser environments.

The exploratory correlation analysis was conducted using the operational metrics extracted from the evaluated browser extensions after CRX extraction and runtime security analysis procedures.

The exploratory analysis revealed a strong positive relationship between injected JavaScript activity and webpage interaction scope as measured through match patterns ($r = 0.802$). In addition, match-pattern coverage exhibited a strong positive relationship with IndexedDB interaction activity ($r = 0.824$). These observations suggest that extensions with broader runtime interaction behavior may also rely on more extensive browser-side storage mechanisms.

The analysis further identified a moderate positive relationship between the overall permission-risk score and the number of sensitive permissions ($r = 0.475$), indicating that extensions requesting broader permission sets tend to include larger numbers of security-sensitive browser capabilities. In contrast, only a very weak relationship was observed between the overall permission-risk score and external communication exposure ($r = 0.043$). This finding suggests that permission-related exposure and communication complexity represent distinct dimensions of operational security exposure and do not necessarily increase together.

The expanded seven-extension evaluation produced more stable exploratory observations than the initial smaller sample. Although the results remain exploratory, the larger extension set improves comparative coverage and reduces the influence of individual extension-specific behaviors on the reported trends.

Because the analysis was conducted on a limited number of evaluated extensions, the reported correlations should be interpreted as exploratory observations rather than statistically generalizable conclusions. Nevertheless, the findings provide useful insights regarding operational interaction trends and browser-centric exposure characteristics within password manager browser extensions.

7. Discussion

The findings of this study demonstrate that security exposure remains an important concern in browser-integrated password management systems despite the use of client-side encryption mechanisms. The experimental analysis revealed substantial differences in permission exposure, runtime interaction behavior, browser-side storage interaction, and external communication complexity across the evaluated password manager browser extensions. The findings additionally support the importance of evaluating password managers through multiple security dimensions rather than relying exclusively on cryptographic protection mechanisms. While encryption remains essential for protecting stored credentials, operational exposure can also emerge through browser permissions, runtime interaction behaviour, browser-side persistence mechanisms, and synchronizationrelated communication pathways.

The permission analysis demonstrated that several extensions require elevated browser privileges to support synchronization, autofill functionality, runtime credential handling, and browser integration operations. Bitwarden demonstrated the highest overall operational exposure index, followed by Keeper and RoboForm. NordPass exhibited the lowest overall exposure score among the evaluated extensions. These findings indicate noticeable differences in permissionrelated exposure across password-manager architectures. These findings are consistent with previous studies indicating that browser extensions frequently request permissions exceeding minimal operational requirements (Picazo-Sanchez et al., 2022). The results additionally support prior discussions regarding browser exposure and browser interaction risks associated with privileged browser extensions (K. Wang et al., 2022; Zahid et al., 2021).

However, the findings indicate that browser security behavior cannot be evaluated solely through permission counts. Although Bitwarden demonstrated the highest operational exposure index, it simultaneously exhibited relatively limited runtime interaction activity compared with Dashlane and NordPass. Conversely,

NordPass demonstrated broader webpage interaction behavior, while RoboForm exhibited the largest external communication footprint. Proton Pass displayed comparatively lower communication exposure despite maintaining a relatively high permission-risk score. These observations suggest that password manager browser extensions rely on substantially different integration and synchronization strategies within browser ecosystems. These observations suggest that password manager browser extensions rely on different integration strategies within browser ecosystems. Unlike previous studies that primarily focused on isolated permission analysis, malicious extension behavior, or browser vulnerability assessment (Picazo-Sanchez et al., 2022; K. Wang et al., 2022), the current analysis combines permission exposure, runtime interaction, browser-side storage behavior, and synchronization-related communication behavior within a unified operational evaluation framework.

The runtime injection analysis demonstrated that Dashlane and NordPass exhibited broader runtime webpage interaction compared with Bitwarden and LastPass. Previous studies highlighted that browser extensions may significantly influence browser behavior because of direct interaction with webpages, browser APIs, and runtime browser components (Jin et al., 2024; K. Wang et al., 2022). The current findings extend these observations by showing that interaction complexity differs substantially across password manager browser extensions.

The browser-side storage analysis additionally revealed substantial variation in persistence behavior and browser-side interaction mechanisms. The findings also highlight broader application-level security exposure considerations. Similar to other application ecosystems, browser-integrated password managers operate within complex software environments that involve persistent storage.

Table 8: Operational Exposure Observations and Security Implications

Observation	Potential Security Implication
High injected JavaScript activity	Increased runtime webpage interaction exposure and expanded DOM interaction surface
Large external URL references	Broader synchronization-related communication behavior and increased external interaction pathways
Elevated sensitive permissions	Increased privileged browser access and operational attack surface expansion
Extensive browser-side storage interaction	Increased persistence-related exposure and local operational dependency

external communication channels, user-interaction mechanisms, and privileged access to sensitive information. These operational characteristics may increase exposure pathways even when strong credential-protection mechanisms are deployed. Consequently, evaluating password-manager security requires consideration of both credential protection and application-level exposure behavior. Keeper demonstrated the highest overall storage interaction activity, while LastPass exhibited the highest localStorage interaction frequency among the evaluated extensions. NordPass demonstrated the highest IndexedDB interaction frequency, closely followed by Keeper. These observations suggest substantial architectural diversity in browser-side persistence and credential-management strategies. These observations suggest that password manager browser extensions rely on different browser-side persistence architectures and storage strategies.

The findings suggest that password manager extensions exhibit several interacting exposure characteristics rather than a single isolated behavior. To further support operational interpretation of the experimental findings, Table 8 summarizes several observed browser-extension behaviors together with their potential cybersecurity implications within browser-based authentication environments. Some extensions demonstrated higher permission sensitivity, while others demonstrated broader runtime interaction or synchronization-related communication behavior. This observation is important because many previous studies focused primarily on permission analysis, browser vulnerabilities, malware detection, or isolated browser-extension risks without integrating multiple runtime interaction dimensions within unified browser-centric evaluation environments (Picazo-Sanchez et al., 2022; Chalyi et al., 2025; K. Wang et al., 2022). The current study extends prior work by experimentally combining permission analysis, runtime interaction assessment, browser-side storage evaluation, and communication exposure analysis within a single operational cybersecurity framework.

The external communication analysis further demonstrated substantial differences in synchronization-related interaction complexity across the evaluated extensions. RoboForm demonstrated the largest number of external URL references, followed by Keeper, NordPass, and Dashlane. In contrast, Proton Pass exhibited the smallest external communication footprint among the evaluated extensions. Although these findings do not necessarily indicate insecure communication behavior, they suggest broader communication surfaces and increased synchronization-related interaction complexity within browser-integrated authentication environments. These differences may reflect architectural design variations involving cloud synchronization intensity, distributed credential management strategies,

telemetry integration mechanisms, and browser-session persistence behavior adopted by different password manager ecosystems.

The exploratory correlation analysis additionally revealed several important operational interaction trends. Injected JavaScript activity demonstrated a strong positive relationship with webpage interaction scope as measured through match patterns, while match-pattern coverage also exhibited a strong positive relationship with IndexedDB interaction activity. These observations suggest that extensions with broader runtime interaction behavior may simultaneously rely on more extensive browser-side persistence mechanisms.

The analysis further identified a moderate positive relationship between overall permission-risk scores and sensitive-permission counts, suggesting that extensions requesting broader permission sets often incorporate larger numbers of security-sensitive browser capabilities. However, only a very weak relationship was observed between permission-risk scores and external communication exposure. This observation indicates that permission-related exposure and communication complexity represent different operational characteristics and should be evaluated independently.

The expanded seven-extension evaluation strengthens the robustness of the comparative analysis by reducing the influence of individual extension-specific characteristics. The broader sample provides improved visibility into architectural differences among contemporary password-manager ecosystems and offers a more representative view of browser-centric exposure behavior.

The results additionally support previous studies emphasizing that browserside processing and runtime interaction may still introduce operational exposure despite the deployment of encryption mechanisms (X. Wang et al., 2021; Jubur et al., 2025). Although client-side encryption protects stored credentials, runtime credential handling, synchronization behavior, browser-session persistence, and privileged browser interaction remain important operational security considerations in browser-integrated authentication systems.

The findings suggest that encryption alone may not fully address exposure concerns within browser-integrated password management environments. Browser attack surface characteristics are additionally influenced by permission sensitivity, runtime interaction behavior, synchronization architecture, browserside persistence mechanisms, and communication complexity. This observation aligns with previous research discussing browser-side interaction risks and runtime browser exposure despite the presence of encryption mechanisms (X. Wang et al., 2021; Jubur et al., 2025), while the current work expands the analysis through a broader multidimensional operational evaluation perspective.

Overall, the study emphasizes the importance of structured cybersecurity evaluation for browser-based password manager extensions. The proposed multidimensional analysis framework supports comparative evaluation across browserintegrated authentication systems by combining permission exposure analysis, runtime interaction assessment, browser-side storage evaluation, synchronization exposure analysis, and exploratory correlation analysis within unified browser-centric security evaluation environments.

8. Limitations

This study has several limitations that should be considered when interpreting the findings and observations presented in the experimental analysis.

First, the evaluation focuses on seven widely used password manager browser extensions operating primarily within Chromium-based browser environments. Although the selected extensions represent a broader cross-section of widely used browser-integrated password managers, the analyzed sample size remains limited and therefore does not necessarily represent the entire browser extension ecosystem. Consequently, the reported operational relationships and exploratory interaction trends should not be interpreted as universally generalizable conclusions across all password manager architectures or browser platforms.

Second, the study emphasizes security exposure, browser interaction behavior, runtime credential handling, and attack surface analysis rather than formal cryptographic verification or cryptographic algorithm evaluation. The analysis therefore focuses on browser-centric exposure characteristics associated with browser permissions, synchronization behavior, runtime interaction, browserside persistence, and extension communication mechanisms. Existing literature similarly highlighted the importance of cybersecurity evaluation and runtime exposure analysis in modern browser-integrated environments (Picazo-Sanchez et al., 2022; X. Wang et al., 2021).

Third, the experimental evaluation primarily relies on static extension analysis and operational browser interaction assessment. The study does not attempt to exploit real-world zero-day vulnerabilities, compromise commercial password manager infrastructures, or perform offensive penetration testing against evaluated products. Consequently, dynamically triggered behaviors, environmentspecific runtime conditions, obfuscated execution paths, or browser interactions activated only

during real-world user activity may not be fully captured within the current experimental analysis. Similarly, the analysis does not directly intercept real user credentials or conduct malicious browser-session exploitation experiments. The goal of the study is therefore to evaluate exposure characteristics rather than demonstrate practical credential compromise scenarios.

Fourth, the runtime exposure analysis was conducted within controlled experimental environments and may not fully represent all real-world deployment conditions, enterprise authentication infrastructures, or organization-specific browser security policies. Browser permission models, synchronization architectures, browser APIs, and extension ecosystems continuously evolve over time, which may influence operational exposure behavior in future browser versions and extension releases.

Fifth, the exploratory correlation analysis was conducted using a limited number of evaluated extensions. Although the observed operational relationships provide useful insights regarding browser interaction complexity, synchronization behavior, and runtime exposure characteristics, the reported correlations should be interpreted as exploratory observations intended to highlight operational interaction tendencies rather than statistically generalizable causal relationships.

Finally, the study focuses specifically on browser-integrated password manager extensions and does not evaluate standalone desktop password managers, enterprise password governance systems, mobile password management environments, or cloud-native authentication infrastructures. Future work may therefore extend the proposed cybersecurity evaluation framework to broader authentication ecosystems and cross-platform password management environments.

9. Conclusion

This study presented a security and attack-surface analysis of password manager browser extensions operating within modern browser environments. The analysis focused on browser permissions, runtime credential handling, browser-session interaction, synchronization behavior, browser-side storage interaction, and external communication exposure associated with browser-integrated password management systems.

The experimental evaluation of seven widely used password manager browser extensions showed substantial differences across browser-related security characteristics. The findings showed that some extensions relied more heavily on privileged browser permissions, while others demonstrated broader runtime webpage interaction, synchronization-related communication behavior, operational browser attack surface expansion, or browser-side storage interaction behavior. The expanded evaluation additionally demonstrated that extensions exhibiting lower permission exposure may still present broader runtime interaction, storage interaction, or communication complexity, reinforcing the need for multidimensional security assessment.

The results additionally demonstrated that client-side encryption alone does not fully eliminate runtime security risks during active browser operation. Runtime credential processing, browser-session persistence, extension interaction, synchronization mechanisms, and browser integration remain important security considerations even when strong encryption mechanisms are deployed.

To support structured browser-centric evaluation, this study proposed a multidimensional security analysis framework integrating permission exposure analysis, runtime interaction evaluation, browser-side storage analysis, synchronization exposure assessment, and exploratory correlation analysis. The proposed framework supports comparative operational evaluation across multiple password manager browser extensions while emphasizing runtime exposure and attack surface expansion within browser-integrated authentication environments.

The expanded seven-extension evaluation improves the representativeness of the analysis and provides broader visibility into architectural differences among contemporary browser-based password-management ecosystems.

Overall, the study highlights the importance of evaluating password manager browser extensions from both cryptographic and browser-interaction perspectives. The findings further demonstrate the importance of multidimensional browser-security evaluation for understanding operational exposure characteristics in modern authentication environments.

10. References

Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). Password Managers - It's All about Trust and Transparency. Future Internet. doi: 10.3390/fi12110189

Amro, A., & Gkioulos, V. (2022). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. Int. J. Inf. Sec.. doi: 10.1007/s10207-022-00638-y

Amro, A., Gkioulos, V., & Katsikas, S. (2023, mar 13). Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework. ACM Transactions on Privacy and Security,

26(2), 1–33. Retrieved from http://dx.doi.org/10.1145/3571733 doi: 10.1145/3571733

Asif, M., Lodhi, R., Sarwar, F., & Ashfaq, M. (2023). Dark side whitewashes the benefits of FinTech innovations: a bibliometric overview. International Journal of Bank Marketing. doi: 10.1108/ijbm-10-2022-0438

Atlam, H. F., Azad, M. A., Alassafi, M., Alshdadi, A. A., & Alenezi, A. (2020). Risk-Based Access Control Model: A Systematic Literature Review. Future Internet. doi: 10.3390/fi12060103

Bitton, R., Maman, N., Singh, I., Momiyama, S., Elovici, Y., & Shabtai, A. (2021). Evaluating the Cybersecurity Risk of Real-world, Machine Learning Production Systems. ACM Computing Surveys. doi: 10.1145/3559104

Butnaru, A. M., Mylonas, A., & Pitropakis, N. (2021). Towards

Lightweight URL-Based Phishing Detection. Future Internet. doi: 10.3390/fi13060154

Chalyi, O., Driaunys, K., & Rud˙zionis, V. (2025). Assessing Browser Security: A Detailed Study Based on CVE Metrics. Future Internet. doi:10.3390/fi17030104

Chandna, V., & Tiwari, P. (2021). Cybersecurity and the new firm: surviving online threats. Journal of Business Strategy. doi: 10.1108/jbs-08-20210146

Cheng, X., Cai, Z., Wang, Z., Dong, Y., & Li, W. (2026, apr 30). A belief rule base method for modeling latent states with uncertainty in Chrome extension risk assessment. Engineering Research Express, 8(9), 095211.

Retrieved from http://dx.doi.org/10.1088/2631-8695/ae62d1 doi: 10.1088/2631-8695/ae62d1

Cornwell, N., Bilson, C., Gepp, A., Stern, S., & Vanstone, B. (2022). The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors. Journal of the Operational Research Society. doi: 10.1080/01605682.2022.2041373

Eckhart, M., Ekelhart, A., & Weippl, E. (2022). Automated Security Risk Identification Using AutomationML-Based Engineering Data.

IEEE Transactions on Dependable and Secure Computing. doi:10.1109/tdsc.2020.3033150

Ganin, A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Analysis. doi:10.1111/risa.12891

Gupta, R., Shankar, R., Lai, K.-H., & Kumar, A. (2023, jan 4). Risk profiling of food security impediments using decision maker's behavioural preference towards operational risk management. Annals of Operations Research, 348(2), 937–972. Retrieved from http://dx.doi.org/10.1007/s10479-022-05148-7 doi: 10.1007/s10479-022-05148-7

Jin, B., Li, H., & Zou, Y. (2024). Impact of extensions on browser performance: An empirical study on google chrome. Empirical Software Engineering. doi: 10.1007/s10664-025-10633-1

Jubur, M., Shrestha, P., & Saxena, N. (2025). An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools. ACM Computing Surveys. doi: 10.1145/3711117

Kennison, S., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity:

Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. Frontiers in Psychology. doi:10.3389 2020.546546/fpsyg.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021, jun 18). The Role of User Behaviour in Improving Cyber Security Management. Frontiers in Psychology, 12. Retrieved from http://dx.doi.org/10.3389/fpsyg.2021.561011 doi: 10.3389/fpsyg.2021.561011

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: utility of communication privacy management theory. Current Opinion in Psychology. doi: 10.1016/J.COPSYC.2019.08.009

Picazo-Sanchez, P., Ortiz-Martin, L., Schneider, G., & Sabelfeld, A. (2022). Are chrome extensions compliant with the spirit of least privilege? Interna-

tional Journal of Information Security. doi: 10.1007/s10207-022-00610-w

Saadi, Z. M., Sadiq, A. T., Akif, O. Z., & Farhan, A. K. (2024). A Survey:

Security Vulnerabilities and Protective Strategies for Graphical Passwords. Electronics. doi: 10.3390/13153042 electronics

Senna, P. P., Reis, A. d. C., Castro, A., & Dias, A. (2020). Promising research fields in supply chain risk management and supply chain resilience and the gaps concerning human factors: A literature review. Work. doi: 10.3233/WOR-203298

Smart, M. A., Sood, D., & Vaccaro, K. (2022). Understanding Risks of Privacy Theater with Differential Privacy. Proc. ACM Hum. Comput. Interact.. doi: 10.1145/3555762

Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter

for operational risk exposure? Technological forecasting & social change. doi: 10.1016/j.techfore.2023.122919

Wang, K., Ling, Y., Zhang, Y., Yu, Z., Wang, H., Bai, G., ... Dong, J. S. (2022). Characterizing Cryptocurrency-themed Malicious Browser Extensions. Proceedings of the ACM on Measurement and Analysis of Computing Systems. doi: 10.1145/3570603

Wang, P., Boodraj, M., & Baskerville, R. (2025). Beyond passwords: A review of the hidden risks in two-factor authentication. Journal of Systems and Information Technology, 28(2), 173-202. Retrieved from https://www.sciencedirect.com/science/article/pii/S1328726525000254 doi: https://doi.org/10.1108/JSIT-03-2025-0140

Wang, X., Du, Y., Wang, C., Wang, Q., & Fang, L. (2021). Webenclave: Protect Web Secrets From Browser Extensions With Software Enclave. IEEE Transactions on Dependable and Secure Computing. doi: 10.1109/TDSC.2021.3081867

Wiefling, S., Jørgensen, P. R., Thunem, S., & Iacono, L. (2022). Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. ACM Transactions on Privacy and Security. doi: 10.1145/3546069

Zahid, M., Inayat, I., Daneva, M., & Mehmood, Z. (2021). Security risks in cyber physical systems-A systematic mapping study. J. Softw. Evol. Process.. doi: 10.1002/smr.2346